QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$. Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸν ις̄ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ις̄ λείψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸν τετράγωνον ἀπὸ ςς̄. ὅσων δή ποτε λείψει τοσούτων μο ὅσων ἐστὶν ἡ τῶν ις̄ μο πλευρά. ἔστω ςς̄ β̄ λείψει μο δ̄. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ̄ μο ις̄ λείψει ςς̄ ις̄. ταῦτα ἴσα μονάσι ις̄ λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε̄ ἴσαι ἀριθμοῖς ις̄. καὶ γίνεται ὁ ἀριθμὸς ις̄ πέμπτων. ἔσται ὁ μὲν σνς̄ εἰκοστοπέμπτων. ὁ δὲ ρμδ̄ εἰκοστοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοστόπεμπτα, ἤτοι μονάδας ις̄. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Είναι αδύνατον μια κυβική δύναμη να γραφεί ως άθροισμα δυο κυβικών δυνάμεων ή μια τέταρτη δύναμη να γραφεί ως άθροισμα δύο τέταρτων δυνάμεων και γενικά οποιαδήποτε δύναμη μεγαλύτερη του τετραγώνου είναι αδύνατον να γραφεί ως άθροισμα ίδιων δυνάμεων. Έχω μια πραγματικά υπέροχη απόδειξη της πρότασης, που όμως δε χωρά σ' ένα τόσο στενό περιθώριο.

Pierre de Fermat 1601-1665

Το θεώρημα του Fermat για N=3

Αρχικές παρατηρήσεις

Για την απόδειξη του θεωρήματος Fermat στα πλαίσια της Αλγεβρικής Θεωρίας Αριθμών, θα δουλέψουμε στο δακτύλιο $\mathbb{Z}[\zeta_3]$ όπου ζ_3 είναι η κυβική ρίζα της μονάδας $\zeta_3=\frac{-1+\sqrt{-3}}{2}=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$.

Είναι $\mathbb{Z}[\zeta_3]=\{\ \alpha+\beta\zeta_3\ /\ \alpha,\beta\in\mathbb{Z}\ \}$. Πολύ εύκολα φαίνεται ότι $\mathbb{Z}[\sqrt{-3}]\subset\mathbb{Z}[\zeta_3]$. Ισχύει βέβαια ότι $\zeta_3^3=1$, $\zeta_3^2+\zeta_3+1=0$, $\overline{\zeta_3}=\zeta_3^2$. Αν $w=\alpha+\beta\zeta_3$ είναι αριθμός του δακτυλίου $\mathbb{Z}[\zeta_3]$ ορίζουμε ως νόρμα του αριθμού τον αριθμό $N(w)=w\overline{w}=\alpha^2-\alpha\beta+\beta^2$. Προφανώς $N(w)\in\mathbb{Z}$ και ισχύει η πολλαπλασιαστική ιδιότητα: $N(zw)=N(z)N(w)$.

Τα αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Z}[\zeta_3]$ καλούνται και μονάδες. Έτσι αν u είναι μια μονάδα θα πρέπει να υπάρχει κάποιο άλλο στοιχείο του $\mathbb{Z}[\zeta_3]$ ώστε $uu'=1$. Παίρνοντας νόρμες προκύπτει $N(u)N(u')=N(1)=1$. Άρα θα πρέπει $N(u)=1 \Leftrightarrow \alpha^2-\alpha\beta+\beta^2=1 \Leftrightarrow (\alpha-\frac{\beta}{2})^2+\frac{3\beta^2}{4}=1$. Αφού λοιπόν θα πρέπει $\frac{3\beta^2}{4}\leq 1$ θα είναι β=0 ή β=1 ή β=-1 και αντιστοίχως οι τιμές του α θα είναι α=±1, α=0 ή α=1, α=0 ή α=-1. Έτσι τελικά προκύπτει ότι το σύνολο των μονάδων του δακτυλίου $\mathbb{Z}[\zeta_3]$ είναι το σύνολο $U=\{\pm1,\pm\zeta_3,\pm\zeta_3^2\}$. Στα παρακάτω για τυπογραφικούς λόγους θα συμβολίζουμε την τρίτη ρίζα της μονάδας ζ_3, απλά ως ζ. Έτσι θα είναι $\zeta=\frac{-1+\sqrt{-3}}{2}$, οπότε $\sqrt{-3}=2\zeta+1$.
Αν η νόρμα του αριθμού w είναι πρώτος φυσικός αριθμός, τότε και ο w είναι πρώτος στο δακτύλιο $\mathbb{Z}[\zeta_3]$. Πράγματι αν w=zk για κάποιους ακεραίους του $\mathbb{Z}[\zeta_3]$, τότε N(w)=N(z)N(k). Αφού N(w) είναι πρώτος θα έχουμε είτε N(z)=1, είτε N(k)=1 δηλαδή είτε z μονάδα είτε k μονάδα του $\mathbb{Z}[\zeta_3]$. Άρα ο w είναι πρώτος. Έτσι ο αριθμός 1-ζ είναι πρώτος αφού N(1-ζ)=3.

Ο δακτύλιος $\mathbb{Z}[\zeta_3]$ είναι ευκλείδειος δακτύλιος. Έτσι αν δοθούν οι αριθμοί $w,z\in\mathbb{Z}[\zeta_3]$ με $z\neq0$, υπάρχουν ακέραιοι $\pi,\upsilon\in\mathbb{Z}[\zeta_3]$ τέτοιοι ώστε $w=z\pi+\upsilon$ με $\upsilon=0$ ή $N(\upsilon)<N(z)$. Από την Άλγεβρα είναι γνωστό ότι ένας ευκλείδειος δακτύλιος είναι περιοχή κυρίων ιδεωδών και κατά συνέπεια δακτύλιος με μονοσήμαντη ανάλυση.

Το σύνολο πηλίκο $\mathbb{Z}[\zeta_3]/2\,\mathbb{Z}[\zeta_3]=\{0,1,\zeta,1+\zeta\}$, μ'άλλα λόγια τα δυνατά υπόλοιπα της διαίρεσης ενός αριθμού w του $\mathbb{Z}[\zeta_3]$ με το 2 είναι ένας από τους αριθμούς του συνόλου $\{0,1,\zeta,1+\zeta\}$, δηλαδή $w\equiv0$ mod2 ή $w\equiv1$ mod2 ή $w\equiv\zeta$ mod2 ή $w\equiv(1+\zeta)$ mod2.
Εύκολα φαίνεται ότι $w^3\equiv0$ ή 1 ή -1 mod2
Για τις μονάδες του $\mathbb{Z}[\zeta_3]$ έχουμε $\pm1\equiv1$ mod2, $\pm\zeta\equiv\zeta$ mod2, $\pm\zeta^2\equiv(1+\zeta)$ mod2.

Η απόδειξη του θεωρήματος Fermat θα γίνει με απαγωγή σε άτοπο. Θα υποθέσουμε ότι υπάρχει λύση (χ,ψ,ω) της εξίσωσης $\chi^3+\psi^3=\omega^3$ (*) με $\chi\psi\omega\neq0$ και $\max\{|\chi|,|\psi|,|\omega|\}$ ελάχιστο, και θα οδηγηθούμε σε άτοπο.

- χ,ψ,ω είναι πρώτοι μεταξύ τους κατά ζεύγη, αφού αν ο λ διαιρεί δυο από τους χ,ψ,ω τότε θα διαιρεί και τον τρίτο. Έτσι η τριάδα ($\left|\frac{\chi}{\lambda}\right|, \left|\frac{\psi}{\lambda}\right|, \left|\frac{\omega}{\lambda}\right|$) θα είναι επίσης λύση της (*) με $\max\{\left|\frac{\chi}{\lambda}\right|, \left|\frac{\psi}{\lambda}\right|, \left|\frac{\omega}{\lambda}\right|\} < \max\{|\chi|,|\psi|,|\omega|\}$.
- Δίχως βλάβη της γενικότητας μπορούμε να υποθέσ0υμε ότι χ άρτιος και ψ,ω περιττοί. (Αν χ περιττός και ψ άρτιος η τριάδα (ψ,χ,ω) είναι επίσης λύση, ενώ αν ω άρτιος και χ,ψ περιττοί, η τριάδα (ω,-ψ,χ) είναι επίσης λύση).
- $\chi^3+\psi^3=\omega^3 \Leftrightarrow \chi^3=\omega^3-\psi^3 \Leftrightarrow \chi^3=(\omega-\psi)(\omega-\zeta\psi)(\omega-\zeta^2\psi) \Leftrightarrow$ $\boldsymbol{\chi^3=(\omega-\psi)(\omega-\zeta\psi)(\omega-\bar{\zeta}\psi)}$ **(1)**
- Αν ένας πρώτος ρ διαιρεί δυο από τους αριθμούς ω-ψ, ω-ζψ, $\omega-\bar{\zeta}\psi$ τότε είναι ρ=(1-ζ)·μονάδα. Πράγματι, αν ρ/ω-ψ και ρ/ω-ζψ τότε ρ/ψ(1-ζ). Ο ρ δεν μπορεί να διαρεί τον ψ γιατί τότε επίσης ρ/ω άτοπο σύμφωνα με την πρώτη παρατήρηση. Θα είναι επομένως ρ/1-ζ και αφού 1-ζ πρώτος θα έχουμε τελικά ότι ρ=(1-ζ)·μονάδα. Αν ρ/ω-ψ και $\rho/(\omega-\bar{\zeta}\psi)$ τότε $\rho/\psi(1-\bar{\zeta}) \Leftrightarrow \rho/(\zeta\bar{\zeta}-\bar{\zeta}) \Leftrightarrow$ ρ/(1-ζ) γιατί $\bar{\zeta}$ είναι μονάδα, οπότε και πάλι ρ=(1-ζ)·μονάδα. Αν τέλος ρ/ω-ζψ και $\rho/(\omega-\bar{\zeta}\psi)$ τότε $\rho/\psi(\zeta-\bar{\zeta}) \Leftrightarrow \rho/\psi(\zeta^3-\zeta^2\bar{\zeta}) \Leftrightarrow \rho/\psi(1-\zeta)$ και παρομοίως προκύπτει ρ=(1-ζ)·μονάδα.
- $(1-\zeta)^3=1+\zeta^2-2\zeta=-\zeta-2\zeta=-3\zeta$ άρα $3=(1-\zeta)^2(-\bar{\zeta})$ (2).

Πρώτη περίπτωση: Αν $3 \nmid \chi$

Τότε επίσης $1-\zeta \nmid \chi$ (Διαφορετικά 1-ζ/χ οπότε $(1-\zeta)^2/\chi$ δηλαδή $3/\chi^2$ άρα 3/χ). Οι αριθμοί ω-ψ, ω-ζψ, $\omega-\bar{\zeta}\psi$ είναι πρώτοι μεταξύ τους (γιατί διαφορετικά για τον κοινό πρώτο διαιρέτης τους το 1-ζ θα είχαμε (1-ζ)/χ).
Από τη σχέση $\boldsymbol{\chi^3=(\omega-\psi)(\omega-\zeta\psi)(\omega-\bar{\zeta}\psi)}$ **(1)** προκύπτει ότι κάθε παράγοντας του δεξιού μέλους της (1) θα είναι το γινόμενο ενός κύβου επί μια μονάδα.
Αν $\omega-\psi=\beta^3\mu$ τότε $(\omega-\psi)^2=|\omega-\psi|^2=|\beta^3\mu|^2=(\beta\bar{\beta})^3(\mu\bar{\mu})^3=(\beta\bar{\beta})^3\in\mathbb{Z}$.
Μπορούμε λοιπόν να γράψουμε $\omega-\psi=\gamma^3$ όπου $\gamma\in\mathbb{Z}$.
Επίσης $\omega-\zeta\psi=\delta^3\mu'$ όπου μ΄ μονάδα. Επειδή $\omega-\zeta\psi\equiv(1-\zeta)\ \mathrm{mod}2 \equiv (1+\zeta)\mathrm{mod}2 \equiv \pm\bar{\zeta}\ \mathrm{mod}2$, θα είναι $\mu'=\pm\bar{\zeta}$ κι έτσι μπορούμε να γράψουμε $\omega-\zeta\psi=\delta^3\bar{\zeta}$.

Συνοψίζοντας θα έχουμε $\begin{cases}\omega-\psi=\gamma^3\\ \omega-\zeta\psi=\delta^3\bar{\zeta}\\ \omega-\bar{\zeta}\psi=\bar{\delta}^3\zeta\end{cases}$ (3)

Αν θέσουμε δ=α+βζ, τότε $\delta^3=\alpha^3+\beta^3+3\alpha^2\beta+3\alpha\beta^2\zeta^2=\alpha^3-3\alpha\beta^2+\beta^3+(3\alpha^2\beta-3\alpha\beta^2)\zeta$ (4) έτσι αφού $\omega-\zeta\psi=\delta^3\bar{\zeta}$ θα είναι $\zeta\omega-\zeta^2\psi=\delta^3 \Leftrightarrow \psi+(\omega+\psi)\zeta=\delta^3$ (5). Από τις (4),(5) θα έχουμε:

$$\begin{cases}\psi=\alpha^3-3\alpha\beta^2+\beta^3\\ \psi+\omega=3\alpha^2\beta-3\alpha\beta^2\end{cases} \Leftrightarrow \begin{cases}\psi=\alpha^3-3\alpha\beta^2+\beta^3\\ \omega=-\alpha^3+3\alpha^2\beta-\beta^3\end{cases} \quad (6)$$

Θα είναι επομένως $\omega-\psi=-2\alpha^3-2\beta^3+3\alpha^2\beta+3\alpha\beta^2=(\alpha+\beta)(2\alpha-\beta)(2\beta-\alpha)$ κι έτσι

$$\gamma^3=(\alpha+\beta)(2\alpha-\beta)(2\beta-\alpha) \quad (7)$$

Είναι εύκολο να δούμε ότι οι ακέραιοι α+β,2α-β,2β-α είναι πρώτοι μεταξύ τους ανά δύο. Σύμφωνα επομένως με την (7) ο καθένας τους οφείλει να είναι τέλειος κύβος.

Θα υπάρχουν λοιπόν ακέραιοι Χ, Ψ, Ω τέτοιοι ώστε $\begin{cases} \alpha+\beta=X^3 \\ 2\beta-\alpha=\Psi^3 \\ 2\alpha-\beta=\Omega^3 \end{cases}$ (8)

Βρίσκουμε λοιπόν $\Psi^3+\Omega^3=X^3$ δηλαδή η τριάδα (Ψ,Ω,X) είναι επίσης λύση της (*). Αφού $X^3,\Psi^3,\Omega^3/\omega-\psi/\chi$ θα είναι $|X|,|\Psi|,|\Omega|<|\chi|$ ($\chi^3=(\omega-\psi)(\omega^2+\omega\psi+\psi^2)$, $\omega^2+\omega\psi+\psi^2>1$ άρα $|\omega-\psi|<|\chi|^3$). Θα έχουμε έτσι $|X|,|\Psi|,|\Omega|<|\chi| \leq \max\{|\chi|,|\psi|,|\omega|\}$ άρα και $\max\{|X|,|\Psi|,|\Omega|\} < \max\{|\chi|,|\psi|,|\omega|\}$ άτοπο.

Δεύτερη περίπτωση: Αν 3/χ

Αφού $3=(1-\zeta)^2(-\bar{\zeta})$ ο πρώτος $1-\zeta$ διαιρεί τον χ. Όμως $\chi^3=(\omega-\psi)(\psi-\zeta\psi)(\omega-\zeta^2\psi)$, επομένως ο $1-\zeta$ θα διαιρεί κάποιον από τους $(\omega-\psi)$, $(\psi-\zeta\psi)$, $(\omega-\zeta^2\psi)$. Είναι όμως $(\omega-\psi)-(\omega-\zeta\psi)=-\psi(1-\zeta)$ και $(\omega-\psi)-(\omega-\zeta^2\psi)=-\psi(2+\zeta)=-\psi(3-1+\zeta)=-\psi[(1-\zeta)^2\zeta^2-(1-\zeta)]$ και επίσης $(\omega-\zeta\psi)-(\omega-\zeta^2\psi)=\psi(\zeta^2-\zeta)=-\psi\zeta(1-\zeta)$, δηλαδή $\omega-\psi\equiv \omega-\zeta\psi \equiv \omega-\zeta^2\psi \bmod(1-\zeta)$, άρα όλοι οι αριθμοί $(\omega-\psi)$, $(\psi-\zeta\psi)$, $(\omega-\zeta^2\psi)$ διαιρούνται με τον $1-\zeta$.

Αν $ord_3(x)=m$ (η μεγαλύτερη δύναμη του 3 που διαιρεί τον χ) και $ord_3(\omega-\psi)=n$ τότε η σχέση $\chi^3=(\omega-\psi)(\psi-\zeta\psi)(\omega-\zeta^2\psi)$ μας δίνει $6m=2n+1+1$. (Πράγματι οι $\omega-\zeta\psi$ και $\omega-\zeta^2\psi$ δεν διαιρούνται με $(1-\zeta)^\kappa$ για $\kappa>1$ αφού το 3 θα διαιρούσε αυτούς τους αριθμούς και αν πχ $\omega-\zeta\psi=3(\alpha+\beta\zeta)$ με $\alpha,\beta \in \mathbb{Z}$ τότε $\omega=3\alpha$ και $\psi=-3\beta$ άτοπο, ενώ αν $\omega-\zeta^2\psi=3(\alpha+\beta\zeta)$ τότε $\omega+\psi=3\alpha$ και $\psi=3\beta$ άτοπο και πάλι αφού $\omega\wedge\psi=1$).

Η σχέση $6m=2n+2$ δίνει $3m=n+1$ οπότε $n\geq 2$. Θα έχουμε λοιπόν:

$\omega-\psi=9\gamma$ με $\gamma \in \mathbb{Z}$

$\omega-\zeta\psi=(1-\zeta)\kappa$

$\omega-\zeta^2\psi=(1-\zeta^2)\bar{\kappa}$ με $\kappa \in \mathbb{Z}[\zeta]$. Είναι $\zeta^2=\bar{\zeta}$.

Θα έχουμε λοιπόν $\chi^3=9\gamma(1-\zeta)(1-\bar{\zeta})\kappa\bar{\kappa} \Leftrightarrow \chi^3=9\gamma 3\,\kappa\bar{\kappa} \Leftrightarrow (\frac{\chi}{3})^3=\gamma\kappa\bar{\kappa}$.

Οι αριθμοί γ, κ, $\bar{\kappa}$ δεν έχουν κανένα κοινό πρώτο διαιρέτη μεταξύ τους γιατί διαφορετικά αυτός θα όφειλε να είναι της μορφής $\alpha=(1-\zeta)\cdot$μονάδα κι αυτό θα σήμαινε ότι ο $\omega-\zeta\psi$ διαιρείται με τον $(1-\zeta)^\kappa$ με $\kappa>1$. Έτσι συμπεραίνουμε ότι

$\omega-\psi=9\lambda^3$

$\omega-\zeta\psi=u(1-\zeta)\delta^3$

$\omega-\zeta^2\psi=\bar{u}(1-\bar{\zeta})\bar{\delta}^3$. Θα δείξουμε ότι $u=\pm1$.

$\omega-\zeta\psi\equiv(1-\zeta)\bmod 2$, $\omega-\zeta\psi=u(1-\zeta)\delta^3$. Ο κύβος όμως ενός μη μηδενικού στοιχείου του $\mathbb{Z}[\zeta]/2\,\mathbb{Z}[\zeta]$ είναι 1. Δηλαδή $\delta^3\equiv 1 \bmod 2$ οπότε $1-\zeta \equiv u(1-\zeta)\bmod 2$ άρα $u \equiv 1 \bmod 2$ άρα $u=\pm1$. Έτσι μπορούμε να γράψουμε $\begin{cases} \omega-\psi=9\lambda^3 \\ \omega-\zeta\psi=(1-\zeta)\delta^3 \\ \omega-\bar{\zeta}\psi=(1-\bar{\zeta})\bar{\delta}^3 \end{cases}$ (9)

Θέτουμε $\delta=\alpha+\beta\zeta$ με $\alpha,\beta \in \mathbb{Z}$. Τότε $\delta^3=\alpha^3-3\alpha^2\beta+\beta^3+\zeta(3\alpha^2-3\alpha\beta^2) \Leftrightarrow$

$(1-\zeta)\delta^3=\alpha^3+3\alpha^2\beta-6\alpha\beta^2+\beta^3+\zeta(-\alpha^3-\beta^3+6\alpha^2\beta-3\alpha\beta^2)$ και από την (9) προκύπτει

$\omega=\alpha^3+3\alpha^2\beta-6\alpha\beta^2+\beta^3$ και $\psi=\alpha^3+3\alpha\beta^2-6\alpha^2\beta+\beta^3$. Είναι λοιπόν

$\omega-\psi=9\alpha^2\beta-9\alpha\beta^2=9\alpha\beta(\alpha-\beta)$ (10). Αφού $\omega-\psi=9\lambda^3$ προκύπτει ότι $\alpha\beta(\alpha-\beta)=\lambda^3$ (11).

Οι ακέραιοι $\alpha,\beta,\alpha-\beta$ είναι πρώτοι μεταξύ τους ανά δύο (αφού $\omega\wedge\psi=1$), άρα θα υπάρχουν ακέραιοι χ_1,χ_2,χ_3 έτσι ώστε $\alpha=\chi_1^3$, $\beta=\chi_2^3$, $\alpha-\beta=\chi_3^3$ δηλαδή $\chi_1^3+(-\chi_2)^3=\chi_3^3$. Η τριάδα $(\chi_1,-\chi_2,\chi_3)$ είναι λύση της (*) και όπως και στην περίπτωση (Ι)

$\max(|\chi_1|,|\chi_2|,|\chi_3|)<\max(|\chi|,|\psi|,|\omega|)$ άτοπο.

Βιβλιογραφία

1. Fermat Last Theorem - Paulo Ribenboim
2. Number Theory 1, Fermat's Dream – Kazuya Kato, Nobushige Kurokawa, Takeshi Saito
3. An introduction to theory of numbers – Ivan Niven, Herbert Zuckerman, Hungh Montgomery
4. Θεωρία Αριθμών – Δημήτριος Πουλάκης
5. Αριθμοθεωρητικός Λογισμός – Κασαπίδης Γεώργιος